STRATEGY
RESEARCH
PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

# TERRORISM – A NEW AGE OF WAR: IS THE UNITED STATES UP TO THE CHALLENGE?

BY

LIEUTENANT COLONEL DONALD L. BAKER
United States Air Force

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited

USAWC CLASS OF 2002

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

# Terrorism – A New Age of War: Is the United States Up to the Challenge?

by

Lieutenant Colonel Donald L. Baker
US Air Force

Colonel Patrick K. Halton
Project Advisor

The views expressed in this academic research paper are those of the author and do not necessarily reflect the official policy or position of the U.S. Government, the Department of Defense, or any of its agencies.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

# ABSTRACT

AUTHOR: Donald L. Baker

TITLE: Terrorism – A New Age of War: Is the United States Up to the Challenge?

FORMAT: Strategy Research Project

DATE: 09 April 2002 PAGES: 41 CLASSIFICATION: Unclassified

The U.S. is being drawn ever deeper into the war on terrorism. Terrorism is predicted to be the primary threat to the US for the foreseeable future. The recent attacks on the US homeland, the USS Cole bombing, and the US embassy bombings in Africa indicate that the stakes are getting higher and higher. The war in Afghanistan demonstrates to the world our resolve in winning the war. But this is only a first step. The war on terrorism will likely be long term and will not be won easily. This is a new kind of war. It will not only be fought on a traditional battlefield with traditional opponents with traditional weapons. It will also be fought on Main Street America and in cyberspace and it will be fought against opponents we can't see or even envision. It will be won with technology, some of which is yet to be developed. But this war will only be as effective as the policies guiding it. The instruments of power must be wielded in new and different ways to achieve our goals. Significant changes in policies and strategies are required to effectively utilize and synergize all the instruments of power. This paper will evaluate current and evolving policies and trends with respect to counterterrorism.

## TABLE OF CONTENTS

## LIST OF ILLUSTRATIONS

## LIST OF TABLES

## TERRORISM – A NEW AGE OF WAR: IS THE UNITED STATES UP TO THE CHALLENGE?

> We are a country awakened to danger and called to defend freedom. Our grief has turned to anger, and anger to resolution. Whether we bring our enemies to justice, or bring justice to our enemies, justice will be done.
>
> Americans are asking: How will we fight and win this war? We will direct every resource at our command – every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence, and every necessary weapon of war – to the disruption and defeat of the global terror network.
>
> —President George W. Bush
> 20 September 2001

On 11 September 2001, 19 terrorists hijacked and crashed four American commercial jetliner aircraft in an unprovoked attack on America striking at the heart of the nation killing thousands of US citizens. President Bush authorized the use of military force on 18 September declaring that it is "necessary and appropriate that the United Stated exercise its right to defend itself and protect United States citizens both at home and abroad."[1]

So begins the world's introduction to the 21st century. To effectively combat terrorism the US will need to use more than the traditional war-fighting military services or the traditional instruments of national power. It will need to synergize all its resource, both military and non-military fully integrating diplomatic, military, economic, and information. Military support must consist of conventional and special operations forces (SOF). However, a great deal of information and support is also available from the Federal Bureau of Investigation (FBI), the Central Intelligence Agency (CIA), Treasury Department, the Immigration and Naturalization Service (INS), and other agencies (including state and local government organizations) which are not normally considered as participants in a war. All of these organizations can contribute to identification and apprehension of terrorists. The US must utilize and coordinate non-traditional elements in combating terrorism. Until the terrorist attacks of 11 September 2001 there was no factor demanding coordination at all levels. To effectively combat terrorism this new war will require novel and innovative ways, ends, and means beginning at the strategic level down through the tactical level.

The war on terrorism will be the war of the 21st century. Just as the terrorist relies on asymmetric means to accomplish his goals, so too must the US resort to asymmetric means to combat terrorism.

## TERRORISM – CRIME OR AN ACT OF WAR?

Defining terrorism is important to determining how it will be addressed. The legal definition of terrorism presents a dilemma. Is terrorism a criminal act or an act of war? There is no universally agreed definition of terrorism. A legal definition is found in the United States Code: "premeditated, politically motivated violence perpetrated against noncombatant targets by subnational groups or clandestine agents."[2] This definition is also adopted by the U.S. Department of State.[3] The Department of Defense (DoD) defines terrorism as the "unlawful violence or threat of violence…intended to coerce or intimidate governments or societies in the pursuit of goals that are generally, political, religious, or ideological."[4] Both these definitions focus on legal terms. Indeed, terrorism is a criminal act. As such it is usually pursued in legal, judicial and diplomatic venues. If viewed from another perspective, Clausewitz defined war as "an act of force to compel our enemies to do our will."[5] Under this definition, terrorism can be considered an act of war. In practice, apprehension and prosecution of terrorists has primarily been the realm of law enforcement and the legal system with additional support efforts including diplomatic and economic sanctions. Hence, the confusion and debate as to what measures are appropriate for terrorist actions.

## COUNTERTERRORISM POLICY

Although Presidential Decision Directive 39 (PDD 39) US Policy on Counterterrorism (originally classified) states that the US will "respond with all appropriate instruments"[6] against organizations and states sponsoring terrorist acts against the US, the primary focus is on legal, diplomatic, and economic means. The Department of State has the responsibility for articulating foreign policy. The current policy, derived from PDD 39, as found in the Department of State Patterns of Global Terrorism – 2000, is:

- Make no concessions to terrorists and strike no deals.
- Bring terrorists to justice for their crimes.
- Isolate and apply pressure on states that sponsor terrorism to force them to change their behavior.
- Bolster the counterterrorism capabilities of those countries that work with the U.S. and require assistance.[7]

The stated policy in the Department of State document also leans heavily toward legal, economic, and diplomatic tools as the preferred solutions, by relying on words such as "justice," "isolate," and "pressure" while omitting any reference to responding "with all appropriate instruments." Although there can be no doubt when bombs are falling that a policy statement is being made, it is better to make such statements in advance in unclassified and public forums. A more strongly worded policy statement identifying that the military is an option that the US is ready and willing to use will serve notice to terrorists and their supporters that such aggressions will not be tolerated and that retribution and punishment will be swift and sure.

## ANTITERRORISM VS. COUNTERTERRORISM

The best defense is a good offense. This axiom is useful not only for athletic competition; it also provides valuable guidance for combating terrorism. Where does one begin to combat terrorism and on what should be the emphasis?

Joint Publication (JP) 1-02 defines antiterrorism (AT) as "defensive measures taken to reduce vulnerability to terrorist attacks."[8] Joint Doctrine Encyclopedia (JDE) further describes antiterrorism as "training and defensive measures that strike a balance among the protection desired, mission, infrastructure, and available manpower and resources."[9]

Counterterrorism (CT) is defined in JP 1-02 as "offensive measures taken to prevent, deter, and respond to terrorism."[10] The JDE describes counterterrorism as "response measures that include preemptive, retaliatory, and rescue operations."[11]

At the outset it might be difficult to understand the difference between AT and CT; both are designed to eliminate the terrorist threat. In general, AT is more reactive and defensive in nature while CT is focused on proactive and offensive measures. The function of AT is to prevent a terrorist from completing an attack on personnel, equipment, and infrastructure or, in the event of an attack, to respond and mitigate loss of life and property. This can be accomplished through training and procedures. The primary function of CT is to identify the terrorist threat and eliminate it before it becomes an imminent threat. CT can also include retaliation and rescue, as necessary. An example of AT would be identifying a terrorist as he attempted to board an airliner while CT would eliminate the terrorist long before boarding the aircraft.

Given that CT is more proactive at earlier identification of the terrorist threat, it follows that CT should be afforded a higher level of emphasis in the US terrorism program. Although AT is important, the focus is at the operational level. For the purposes of this discussion, the operational level is not limited to military activities; it can also include civilian infrastructure vulnerable to terrorist threats. The goal should be to eliminate the threat before reaching the operational level. Therefore, CT is more strategic while AT is focused more at the operational level. Although CT activities can be tactical in nature, the result is strategic. An analogy is the strategic bombing done in WWII to destroy the German ball bearing plants and oil fields. This diminished Germany's strategic ability to prosecute the war before forces could be brought to bear against ground forces.

## WAR ON DRUGS – LESSONS LEARNED

Military planners customarily look at other plans or operations to draw on existing experience or information. In combating terrorism the US can draw on many lessons learned (both good and bad) from the war on drugs. The farmers growing the raw materials, the drug cartels, the transportation methods, the drug dealers, or the end users cannot be considered as individual links in a chain; breaking one of the links will not solve the problem. The situation is more of a network with many interconnecting paths for the flow of drugs (and terrorism); eliminating one node does not collapse the entire network. The war must be considered as a single coordinated operation integrating all resources available with a grand strategy to support the prosecution of the war on terrorism. In the war on drugs the US synergizes law enforcement (LE), intelligence and military operations to combat drugs.

A common thread between the war on drugs and the war on terrorism is that drug money is frequently used as a resource for supporting terrorism. Therefore, eliminating the drug trade also has benefits in reducing terrorism. The policy and legal instruments put into place to freeze or seize assets and resources associated with drugs have served as the basis for similar and expanded efforts in attacking the resources of terrorism.

Conversely, the efforts of the war on terrorism will undoubtedly benefit the war on drugs. Previously the war on drugs still suffered from some stove-piping of information within and rivalry between Federal, State, and local organizations resulting in inefficient operations. One of the results of the war on terrorism will be to eliminate stove-pipes, foster better working relationships, and leverage technology.

## WEAPONS OF MASS DESTRUCTION (WMD)

The National Military Strategy identifies "terrorism, the use or threatened use of WMD, and information warfare"[12] as our greatest asymmetric challenges. The terrorist threat of the future will seek to utilize asymmetric threats to avoid our strengths and attack our weak points. The very technology that has enabled and enhanced our advances and economic progress could prove to be our "Achilles' heel." Technology has allowed for widespread information on WMD. Experts agree that it is no longer a question of "if" terrorist will acquire and use WMD but "when."[13] The adage "kill 10, frighten 10,000," is especially relevant with respect to WMD; terrorists need only to commit a few acts of terrorism to effectively achieve their goals. The very thought of WMD strikes fear into the hearts of people; WMD can be employed anytime, anywhere, both home and abroad. Therefore, WMD is of major concern to the US. Proliferation of WMD elements has increased the possibilities that terrorists will use WMD more frequently. Terrorist organizations are aided by the availability of knowledge, experience, and materials from outside nations. The outside nations include the "axis of evil" (Iran, Iraq, and North Korea) and the former Soviet Union. Intelligence sources conclude that states such as Iran, Iraq, and North Korea, among other nations hostile to the US, have ongoing WMD acquisition and development programs. It is estimated that "at least a dozen countries have or are actively seeking anthrax for use as a biological weapon."[14] These nations could be tempted to export terrorist materials to non-state actors allowing the terrorist organizations to execute the delivery of WMD thus accomplishing the goals of the supporting nation through the surrogate terrorist organization.

The former Soviet Union had an extensive bioweapons program with an annual capacity of 4,500 metric tons of anthrax in addition to smallpox and other deadly viruses; one facility alone had the capability to produce "1.5 tons of weaponized anthrax in 24 hours."[15] The security of most of the facilities where stockpiles are stored is marginal at best and highly susceptible to theft. Additionally, it is estimated that the Soviets employed 60,000 people for their bioweapons projects. With the collapse of the Soviet Union, these people had to find other employment, and many are still unemployed.[16] The Stimson Center in Washington DC estimates that 10,000 former Soviet bioweapons experts are potential sources of technical expertise for terrorist organizations.[17] Indeed, documents found in al Qaeda caves indicate that the terrorists attempted to recruit former Soviet scientists.[18]

The availability of nuclear weapons and weapons grade materials (Uranium (U-235) and Plutonium (Pu-239)) are also a matter of concern. Terrorist organizations can obtain nuclear weapons/materials from several sources:

- The black market (stolen materials/weapons)
- Willing sponsor states (such as Iraq) which already possess the materials, knowledge, experience, equipment, and weapons
- Develop autonomous weapons program

Although the principles of nuclear physics and weapons development are well understood and widely available, the production is complicated and requires specialized equipment and highly skilled personnel. For these reasons it is difficult for terrorist organizations with limited resources and facilities to develop a nuclear weapons capability without external assistance either in the form of black market materials or sponsor states. The security of nuclear weapons and materials in Russia and the former Soviet states is in the same condition as the bioweapons; security is poor and corruption is high making Russia a prime source of black market nuclear materials. In December 2001 members of a criminal gang were arrested in Moscow attempting to sell 2 pounds of stolen U-235.[19] This is only a recent example – arrests in Russia and other European countries abound. The Department of Energy (DOE) estimates that only 8.8 pounds of Pu-239 is necessary for a small nuclear weapon.[20] The good news is that between 1993 and 2000 the number of worldwide thefts of nuclear materials generally decreased; the bad news is that during the same period there was an increasing trend of thefts of low level radioactive materials.[21]

Although radiological weapons are not as destructive as nuclear ones, radioactive materials are more widely available and easier to acquire. In the US alone there are more than 2 million devices that use radioactive materials.[22] The Nuclear Regulatory Commission has reported that over 1,700 instances of lost or stolen radioactive material since 1986. In 1998, 19 vials of radioactive Cesium-137 were reported missing from a hospital in Greensboro, North Carolina. In Russia in November 2001 two men were arrested with stolen radioactive cobalt.[23] Allied forces in Afghanistan discovered documents describing the construction of a "dirty bomb"[24] – conventional explosives wrapped with radiological materials. Such a weapon would have a relatively small effect (when compared to a nuclear device) but the potential psychological and economic impact of a radiological weapon could be devastating.

Chemical weapons are extremely lethal and numerous states have a chemical arsenal. Chemical weapons are difficult for non-state actors to make and employ. As with nuclear and biological threats, the support of sponsor states seems to be the most likely source of chemical weapons for terrorists. The threat of autonomous weapons development by non-state actors should not be discounted as evidenced by the Aum Shinrikyo religious cult sarin gas attack in a Tokyo subway in 1995.

High-yield explosives (such as used in the Oklahoma City and the 1993 World Trade Center bombings) can be manufactured from readily available materials. These weapons tend to be heavy, bulky and difficult to transport through secure checkpoints. Areas with inadequate security are highly vulnerable.

The rapid technological and informational advances that have supported our economy and military technologies have proven to be a double-edged sword by facilitating terrorist activities. It is not easy to control proliferation of WMD information and terrorist communications. Similarly, it is extremely difficult, if not impossible, to guard against all potential avenues of attack. Competing and limited resources prohibit a 100 percent guarantee of protection. Solutions include addressing the sources of proliferation (securing/destroying existing stockpiles and harnessing rogue states), leveraging technologies to provide thè greatest assurance against attack, maximizing intelligence efforts to identify and track WMD, and integrating a cross-flow of information to take full advantage of all available organizations to combat terrorism.

## COMMUNICATION

The war on terrorism will be fought on two broad and diverse fronts: the US homeland and abroad. These two categories will require different rules of engagement (ROE). Two general statements can be made which both fronts will have in common: 1) they will each be fought by coordinating efforts at all levels of the government (to include non-traditional organizations), and 2) changing existing methods of operations will be essential to success. What is unique about these previous statements is that formerly, government agencies have tended to stove-pipe information. The result, at best, has been overlapping redundancies. At worst, the stove-piping has effectively resulted in gaps or seams in information. It is not that there is necessarily an absence of information but more a lack of access to information both horizontally and vertically. Without providing wider access to information, organizations are unable to see the "big picture" and how they can contribute to the war on terrorism.

There is a team-building game that illustrates the benefits of communication and sharing information. Two teams consist of four players each. Each player has his own set of geometrically shaped puzzle pieces and is given the task of creating his own square. He must do this by either using his own pieces or by trading pieces with other players on his team. Some players cannot create squares unless they trade pieces with others while some of the team members are able to create squares with their own pieces without trading. However, for each team member to successfully create a square, all team members (even those with completed squares) have to be willing to share some of their pieces even if it means giving up pieces when they already have a completed square. The difference between the two teams is that one team is allowed to talk while the other team cannot and must resort to other means of communication to exchange puzzle pieces allowing each player to form a square. Invariably, the team that verbally communicates is able to complete the task before the other team. Team members who are able to complete squares with their own pieces are unwilling to exchange pieces unless they can be convinced that they too will end up with a completed puzzle. If the team members cannot communicate it is difficult for them to be convinced that sharing will benefit the entire team. In this exercise the puzzle pieces can be considered data. The game demonstrates that when team members communicate and share information or data they are much more effective. The adage that "information is power" implies that one who has information has power. However, the adage for the information age will need to be "shared information is power." Organizations that effectively share information will have a greater level of coordinated operations and effectiveness, and thus, power. The key is to effectively share information.

## LAW ENFORCEMENT VS. INTELLIGENCE

Statutorily, law enforcement and intelligence activities are separate efforts. The benefit of this division of activities is that this secures US citizens against abuses that can result when the responsibilities for both activities are imbedded within the same organization. Indeed, such abuses were manifested in the 1970s giving rise to the Church and Pike Commissions and resulting in increased congressional oversight. However, this separation also has drawbacks primarily because law enforcement and intelligence information is stove-piped and compartmented leading to a situation where neither organization has a full understanding of the terrorist threat. In an attempt to remedy this situation, Congress developed the USA PATRIOT Act.

## LEGISLATION

The US Congress has enacted several laws that facilitate Federal, State, and local authorities' efforts to combat terrorism, the most significant of which is the USA PATRIOT Act. Additionally, President Bush issued Executive Order 13224 expanding Treasury Department's power to freeze terrorist financial assets. Together, the USA PATRIOT Act and Executive Order 13224 provide significant powers to combat terrorism both at home and abroad.

### USA PATRIOT ACT

Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act providing broad and sweeping powers for the federal government to directly combat terrorism. The act –

- Expands power of law enforcement authorities to monitor electronic communications. (Note: A sunset clause terminates this provision on 31 December 2005 unless otherwise extended by Congress.)
- Adopts measures for the Department of the Treasury to combat money laundering, investigate sources of terrorist funding and freeze financial assets.
- Enhances border protection through coordination and information sharing between the INS, FBI, Department of Justice (DOJ) and DOS.

- Removes obstacles to investigating terrorism, increases information sharing for protection of critical infrastructure, and strengthens criminal laws against terrorism.
- Authorizes the Secretary of Defense (SECDEF) to support the DOJ in activities relating to criminal violations of WMD laws.[25]

The Foreign Intelligence Surveillance Act (FISA) of 1978 allowed LE agencies to seek wiretapping authorization through a streamlined process when spying or terrorism is suspected. The USA PATRIOT Act further broadened the powers granted by FISA. Zacarias Moussaoui, was arrested on 17 August 2001 on immigration charges after seeking training on how to fly, **but not land**, jetliners. The FBI did not seek a wiretapping warrant because they felt there was insufficient evidence. Subsequent to 11 September investigations have led authorities to believe that Moussaoui would have been the 20th hijacker. [26] If the provisions of the PATRIOT Act had been in effect prior to 11 September it would have made it much easier for authorities to attain the necessary electronic surveillance authorization which leads to the possibility that the terrorist acts of 11 September could have been prevented.

## EXECUTIVE ORDER 13224

On 23 September 2001 President Bush signed Executive Order 13224, Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten to Commit, or Support Terrorism, declaring that "we will starve terrorists of funding, turn them against each other, rout them out of their safe hiding places, and bring them to justice."[27] The order "expands the Treasury Department's power to target the support structure of terrorist organizations, freeze the US assets and block the US transactions of terrorists and those who support them, and increased our ability to block US assets of, and deny access to US markets to foreign banks who refuse to cooperate with US authorities to identify and freeze assets abroad."[28] The specific goals are to deny terrorists access to finances, impair their fundraising, and isolate their financial networks. A total of 27 terrorists, terrorist organizations, charitable organizations and corporations are identified in EO 13224[29]; 21 additional organizations and individuals have since been added[30]. This order has been very effective in denying terrorist organization's assets. As of 23 March 2002 a total of $104.8 million in terrorist assets have been blocked by the US ($34.2 million) and 142 other nations ($70.5 million).[31] The success represents a combination of both the economic and diplomatic elements of power.

## CONGRESSIONAL OVERSIGHT

Congressional oversight of law enforcement and intelligence activities is similarly difficult to effect. Oversight includes the ten congressional committees in Table 1, plus an equal or greater number of sub-committees. These committees and sub-committees have broad and disparate roles, responsibilities, and interests. Getting these committees to agree on legislation and oversight responsibilities is very difficult. Each committee derives a certain level of power from its oversight and budgetary responsibilities. Abrogating a portion of that authority to another committee will be perceived as a weakening of the losing committee.

| Purpose | Senate Committee | House Committee |
|---|---|---|
| Foreign relations | Senate Foreign Relations Committee | House International Relations Committee |
| Intelligence | Senate Select Committee on Intelligence | House Permanent Select Committee on Intelligence |
| DoD | Senate Armed Services Committee | House Armed Services Committee |
| Law enforcement | Senate Judiciary Committee | House Judiciary Committee |
| Appropriations | Senate Appropriations Committee | House Appropriations Committee |

TABLE 1 CONGRESSIONAL OVERSIGHT COMMITTEES

There are three distinct (but somewhat overlapping) areas of responsibility involved in the war on terrorism: law enforcement, intelligence, and military activities. LE is primarily the function of the FBI but the DoD may play a supporting role within the limits established by the Posse Comitatus Act. Intelligence activities are conducted by the CIA, the Department of State Bureau of Intelligence and Research (INR), and the various DoD intelligence organizations. Military activities are primarily the responsibility of the DoD but the CIA is playing an increasing role. To be fully effective, all activities must be coordinated both horizontally and vertically. Given the lack of coordinated congressional oversight, it has previously been difficult, if not impossible, to achieve an integrated effort. One suggested solution is to conduct joint congressional hearings or establish a committee (or committees) specifically for the purpose of coordination of LE and intelligence activities.[32] Resolution of this issue will be key to effective coordination not only at the strategic level but can also serve to support both vertical and horizontal efforts.

## HOMELAND SECURITY

On 8 October 2001 President Bush signed an executive order establishing the Office of Homeland Security to be directed by the Assistant to the President for Homeland Security (HLS). The mission of the office is to "develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks."[33]

The Director was given broad responsibilities to coordinate with Federal, State, and local governments and private entities to "detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States."[34] The executive order also established the Homeland Security Council to advise the President on matters relating to homeland security and to coordinate the activities of departments and agencies to ensure "effective development and implementation of homeland security policies."[35] Two of the specific functions of the Council are: 1) review of legal authorities and development of legislative proposals and 2) budget review.[36] The director of the Office of HLS has no specific legal or budgetary authority. As such, his ability to shape and influence the entirety of Federal, State and local terrorism programs will largely depend on his ability to convince the departments and agencies to work together.

## HOMELAND SECURITY FUNDING

The FY 2002 budget, supplemental FY 2002 budget and the proposed FY 2003 budget (see Table 2) underscore the importance of changes in the methods of operations. The FY 2002 Supplemental Budget reflects an increase of 50% over the FY 2002 HLS budget. Moreover, President Bush's FY 2003 proposed budget (an increase of almost 200% over the FY 2002 budget) provides for significant increases for homeland security.

The FY 2003 budget proposes to harness technology to more efficiently manage the shipment of goods freeing border personnel to concentrate on higher priorities. Another proposal is to develop a system for the INS to track the arrival and departure of non-US citizens and to share this information with LE and intelligence communities[37]. This system will improve the ability to deny access to persons who should not be entering the US.

| Item | FY 2002 Enacted | FY 2002 Supplemental | FY 2003 |
|---|---|---|---|
| Supporting First Responders | $291 | $651 | $3,500 |
| Defending Against Biological Terrorism | $1,408 | $3,730 | $5,898 |
| Securing America's Borders | $8,752 | $1,194 | $10,615 |
| Using 21st Century Technology to Defend the Homeland | $155 | $75 | $722 |
| Aviation Security | $1,543 | $1,035 | $4,800 |
| Other Non-DoD Homeland Security | $3,186 | $2,384 | $5,352 |
| DoD Homeland Security (Outside Initiatives) | $4,291 | $689 | $6,815 |
| **Total** ($ in Millions) | $19,626 | $9,758 | $37,702 |
| % Increase from FY 2002 | | 49.72 | 192.10 |

TABLE 2 HOMELAND SECURITY FUNDING[38]

If the Homeland Security items in the proposed FY 2003 President's Budget are approved, it will reflect a strong commitment in the war on terrorism. Together, the technology to facilitate shipment of goods and the INS database will provide significant capabilities to protect the borders and exclude terrorists from entering the US. Keeping terrorists out of the US does not guarantee the safety of US military personnel, civilians, and businesses abroad.

## INS – SECURING THE HOMELAND

While the Intelligence Community can be considered the first line of defense in identifying terrorists and terrorist organizations, the INS is the first line of defense in securing the US homeland against terrorists. Given the vast length of the US border, the numerous ports of entry, the large number of persons entering and exiting the US and the volume of commercial shipping transactions, the task is formidable. Inadequate funding has further exacerbated the situation in that the INS has not been able to maintain the necessary manpower or upgrade and implement information systems which would allow for better management and tracking of immigrants and shipping.

In the past, terrorists have employed a variety of techniques to enter the US from Canada. They have posed as students or easily slipped through the extremely porous border or passed themselves off as tourists or used false passports.[39] Once in the US they are able to carry out their plans with very little chance of being detected.

Managing the sheer volume of persons entering the US presents a daunting task. Of those entering the US legally, the INS is unable to track more than 500,000 foreign students attending US universities. The students range from nuclear engineering students to student pilots. The terrorist who parked the explosive-filled truck under the World Trade Center in 1993 entered the US as a student.[40] Khalid al-Midhar was on the INS "watch list" and being hunted by the FBI when he boarded American Airlines flight 77 which would later crash into the Pentagon.[41] Additionally, the INS is unable to locate more than 3 million foreign nationals who have overstayed their visas. The INS has no record of six of the 19 terrorists who crashed the four aircraft on 11 September although they are believed to have legitimately entered the US. There are an estimated 7 million people in the US illegally.[42]

Similarly, securing the US borders presents a seemingly impossible situation. There are only 334 Border Patrol agents to police the entire 4,000-mile US-Canadian border. Some entry points are closed from midnight to 8 a.m. with only rubber cones blocking entry. In some remote areas there is so much area between the checkpoints that it is easy to walk across the border. Additionally, the INS has only a small staff dedicated to security coordination with LE; manpower is so limited that counterterrorism was not a high priority.

The flow of people and goods is critical to a strong economy. The US shares a 7,500-mile border with Canada and Mexico and an excess of 500 million people, including 330 million non-citizens, enter the US annually. Additionally, 13.4 million truck and rail cars cross into the US and 7,500 foreign-flag ships enter US ports 51,000 times each year.[43] It is difficult to effectively manage this mass of people and vehicles flowing into the US without integrated technology. If the fear of terrorists is allowed to disrupt the flow of goods and services it will result in a direct impact on the US economy. Again, technology must be leveraged to protect our borders, enhance security, and facilitate the efficient flow of commerce.

Subsequent to 11 September the INS and Customs Commissioners are receiving daily intelligence briefings.[44] This provides a necessary link, or vertical integration, between the strategic and operational levels. When the INS and Customs Commissioners weren't included in strategic level briefings, it was not easy for them to understand the true nature of the threat. Without the insight provided by the intelligence briefings it was difficult to properly assess the situation and prioritize resources.

In an effort to streamline the functions of the INS it was announced on 14 November 2001 that the INS would restructure by separating service and enforcement into two separate functions. The Bureau of Immigration Service will provide basic services to immigrants legally entering the US. The Bureau of Immigration Enforcement will be responsible for enforcing immigration laws against immigrants illegally in the US. The restructuring also affects INS regional field offices and will refocus them on either service or enforcement, but not both. It is anticipated that focused enforcement efforts will streamline reporting and investigations that previously hampered border patrol officials. Although the services and enforcement functions will be separated they are intricately linked and will require coordination to effectively administer immigration laws. This relationship will be supported by the INS Chief Information Officer who will be responsible for developing inter-links to not only ensure that services and enforcement are connected but also to share information with other Federal, State, and local government agencies. Finally, the INS will place emphasis on coordinating and cooperating with foreign governments and LE agencies.[45]

## INTELLIGENCE – THE FIRST LINE OF DEFENSE

How do you identify terrorists? Intelligence is the key force multiplier in the war on terrorism. It can be used to locate terrorists and determine plans for terrorist acts. Without intelligence, terrorists can remain in the shadows, darting out and occasionally striking, then moving quickly back to the darkness from which they came. Intelligence is therefore an important CT tool.

### IN THE BEGINNING

Prior to WWII the US paid little attention to intelligence. The attack on Pearl Harbor changed our perspective and intelligence was instantly afforded higher importance. Massive resources were poured into intelligence. The US learned that there were many indications and warnings (I&W) that, if they had been collected, correlated, and analyzed, might have prevented the devastating attack of 7 December 1941.[46] An evaluation of information after the attacks of 11 September seems to point out that indications and warnings were there.[47] But there were insufficient resources available to put the information together in a coherent form. In 1941 it took a direct, unprovoked attack to awaken strategic leaders to realize that intelligence could play a key role in protecting the US. It took another direct unprovoked attack on 11 September 2001 for leaders to relearn the lessons of 1941 that intelligence is not a tool that can be set aside in the background and only supported in time of emergency. It requires constant and devoted attention to ensure that it is responsive to the security of the nation. Now, massive amounts of resources are being dedicated to a revival and restructuring of the intelligence community.

## INTELLIGENCE OVERSIGHT

In an effort to evaluate the intelligence community's response to terrorism, the House Permanent Select Committee on Intelligence (HPSCI) and the Senate Select Committee on Intelligence (SSCI) oversight committees have decided to conduct a joint bipartisan investigation. The investigation will focus only on the intelligence efforts of the last 16 years including the first World Trade Center attack (1993), the Khobar Towers bombing (1996), the US embassy bombings in Kenya and Tanzania (1998), and the USS Cole attack in Yemen (2000). The decision to conduct a joint investigation, in itself, marks a significant change in the method of operations of the Congress and Senate. Although the SSCI (chaired by Senator Bob Graham, (D-FL)) and HPSCI (chaired by Representative Porter Goss (R-FL)) intelligence committees have conducted joint investigations before, they have never done so while being led by members of different political parties.[48] The very fact that the House and Senate are taking this radical approach to intelligence signals that they understand the old way of doing the business of intelligence will need to be reevaluated, perhaps breaking down some barriers that previously prevented a coordinated cross flow of essential information. The signal to all organizations that collect and use intelligence information should be that "business as usual" may not be the best approach and that "out of the box" thinking must be done to better coordinate both within the Intelligence Community and externally with LE and other organizations which can add value to the CT effort.

## THE INTELLIGENCE COMMUNITY

The Director of Central Intelligence (DCI) is responsible for advising the President and the National Security Council on national security intelligence matters. The DCI leads the Intelligence Community (IC) which consists of three broad categories of national level intelligence organizations (see Table 3 and Figure 1). The IC, led by the DCI, is tasked to direct and conduct all national foreign intelligence and counterintelligence activities. However, the DCI has limited powers to force the large bureaucracies of the Intelligence Community (IC) to form together as a seamless entity. He has the ability to provide input to the budget for the IC intelligence activities but once the budget is signed, much like the Director of HLS, he loses the capability to directly influence the priorities except through negotiation with the respective elements. Moreover, he has no authority or control to eliminate information stove-piping.

| Category | Organization(s) |
|---|---|
| Independent Agency | • Central Intelligence Agency (CIA) |
| Department of Defense Elements | • Defense Intelligence Agency (DIA)<br>• National Security Agency (NSA)<br>• Army Intelligence<br>• Navy Intelligence<br>• Air Force Intelligence, Surveillance, and Reconnaissance<br>• Marine Corps Intelligence<br>• National Imagery and Mapping Agency (NIMA)<br>• National Reconnaissance Office (NRO) |
| Departmental Intelligence Elements (other than DoD) | • Federal Bureau of Investigation (FBI)<br>• Department of the Treasury<br>• Department of Energy (DOE)<br>• Department of State (DOS) |

TABLE 3 INTELLIGENCE COMMUNITY

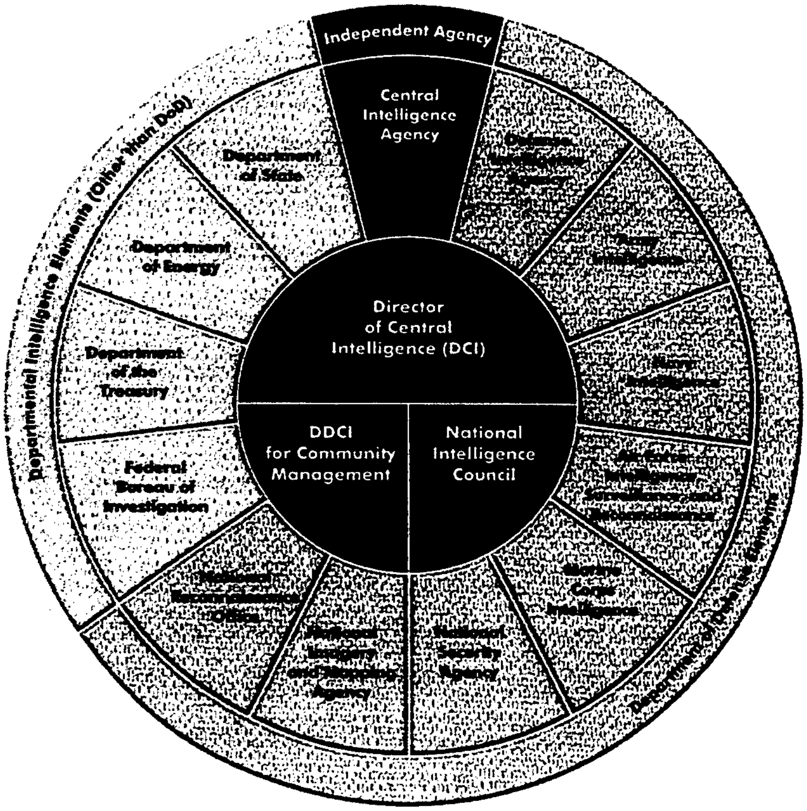
Independent Agency
Central Intelligence Agency
Director of Central Intelligence (DCI)
DDCI for Community Management
National Intelligence Council
Departmental Intelligence Elements (Other than DoD)
Department of State
Department of Energy
Department of the Treasury
Federal Bureau of Investigation
Department of Defense Elements

FIGURE 1 INTELLIGENCE COMMUNITY

A Federal department's ability and/or willingness to share information is dependent more on the emphasis that each organization places on the value of information sharing (insight that shared information is power), on the level of funding provided to support the required technology, and the extent to which the organization perceives a direct benefit. The situation is further complicated in that the emphasis is on national level or strategic intelligence. Prior to the establishment of the Office of HLS there was no single strategic level proponent of a seamless method to coordinate dissemination of intelligence data to the local LE level. Although the DCI is designated as the leader of the IC, his focus is to provide strategic advice to the President. There is no one organization that manages, integrates, and coordinates all levels (strategic, operational, and tactical) of intelligence across the IC. Therefore, true unity of effort is extremely difficult to achieve. Additionally, each intelligence organization has its own focus and priorities which do not necessarily coincide with that of the CIA. The problem is further complicated with respect to the non-DoD federal agencies (the Department of State, the Department of Energy, the Department of Treasury, and the Federal Bureau of Investigation). Each of these organizations have different pieces of information that can contribute to the war on terrorism. However, there is no single organization providing oversight to ensure that information is integrated seamlessly across all levels of the government. There is no common database for information sharing and there are varied levels of emphasis for priority and funding.

## TYPES OF INTELLIGENCE

Intelligence takes many forms to include signals intelligence (SIGINT), imagery intelligence (IMINT), human intelligence (HUMINT), measures and signatures intelligence (MASINT), and open sources intelligence (OSINT). All of these tools can be used to fight terrorism, but there are strengths, limitations, and mitigating factors associated with the various "INTs."

SIGINT, IMINT, and MASINT are highly oriented toward technological methods of collecting and processing. Technological advances have lead to a greater reliance on technical methods and decreased focus and emphasis on HUMINT.[49]

HUMINT has been characterized as the second oldest profession. In biblical times, Joshua employed spies to provide HUMINT prior to invasion of the Promised Land. HUMINT can provide a wealth of information unavailable from any other source. If terrorists take sufficient precautions to minimize their intelligence "signatures" while planning an activity their chances of successfully completing the activity increase. A terrorist organization that limits its SIGINT signature may never be identified. If it operates on a face-to-face basis, no electronic signal is generated thus obviating a primary source of identification. In this instance, only HUMINT can provide information on the true intentions of a terrorist organization. However there are several limitations with HUMINT. The first is that it is more unreliable (i.e. subject to providing false data). The second is that it requires long lead time to develop HUMINT contacts. Over the years the US intelligence focus has shifted to more technologically oriented sources tending to rely on satellite or other resources that can provide "hard" and more consistently reliable data. The result has been a decrease in HUMINT emphasis and capability. However, as we adapt our capabilities, operations, and procedures to further exploit the technical INTs terrorists will learn to minimize their signatures and change their methods to face-to-face, one-on-one communications making HUMINT more important.

Shulsky presents views of former DCIs William Colby and Stansfield Turner that advocate that the world is (or should be) progressing toward the point of making intelligence public and letting the world respond to the situation.[50] Indeed, we are progressing to an open society with a wide proliferation of information. Perhaps making intelligence more widely available will expose terrorists. Conversely, it could force them to change tactics and procedures requiring us (at great expense) to change and refocus our collection methods. The most secure communication is face-to-face in a secure location. All the sophisticated technology possessed by the US cannot guard against such communications. In such situations, human intelligence can provide the only warning of an impending terrorist action.

Operation Enduring Freedom presents a classic dichotomy of technology extremes that provides lessons for intelligence. US ground troops employed 19th century modes of transportation (horses) while employing modern technology (GPS and laser) to target the enemy. Meanwhile, overhead, the Air Force used the oldest aircraft in its inventory, the 40 year-old B-52 aircraft, to drop precision guided munitions. While using all the latest intelligence technologies such as SIGINT, MASINT, and IMINT we must be prepared to be innovative in integrating the oldest intelligence resources (HUMINT).

## COMBATING TERRORISM ABROAD

In some ways, combating terrorism abroad will be much more difficult than fighting terrorism within the US. The US has complete control (at least in theory) over the federal agencies responsible for combating terrorism within the US. However, influencing the US terrorism policy abroad will require complete coordination of all the instruments of national power to persuade other governments to support the war on terrorism. Not only will all the US agencies have to work together, but they will have to do so in a way so as to convince foreign governments to support the US policy. Persuading the foreign governments will present the most problems. There are many different governments requiring varying levels of effort of each instrument of national power.

### MILITARY EFFORTS - TERRORISM IN THE FUTURE

The current war, Operation Enduring Freedom (OEF), is going well. Overall opposition has been relatively light and US casualties lighter still. Activities are now primarily focused on capturing the remaining al Qaeda members and exploring the remaining areas. Civil-military operations and civil affairs will assist the people of Afghanistan to set up a government. It is now time to focus on future operations of the war on terrorism. Where will we go next? Who is the next enemy?

Once the OEF offensive operations are complete, future counterterrorist operations are likely to require a different approach. State sponsors of terrorism are likely to learn the following lessons:

- Covert Support. Former state actors that supported terrorism will realize that overt support of terrorism is extremely dangerous. From the point of view of the state sponsor of terrorism, covert support will become the preferable method of operation. Furthermore, covert terrorist groups will be smaller, more widely dispersed, and harder to detect and penetrate.
- Environment. Terrorists will learn that operating in an open area conducive to a bombing campaign is not favorable to one's health or long term operating ability. Therefore, operating in an urban environment and mixing closely with the civilian population will present a greater challenge to US policymakers seeking to minimize collateral damage.
- Operations. Concentrated operations allows for easier targeting. Therefore, future terrorist operations are more likely to be conducted by widely dispersed cells. Efforts to deal with such operations will necessitate similar counter-tactics requiring more widely dispersed US forces.

If one accepts the previous argument regarding widely placed terrorist cells, the resulting counter-tactic is a reliance on small counter-terrorist teams. The mission and composition of the team will depend on the type of environment.

## PERMISSIVE ENVIRONMENT

A permissive environment can be defined as one in which the host government is friendly or supportive of the US war on terrorism and will allow extradition of terrorists or aggressive prosecution within the host government's legal system. In a permissive environment, the CIA, SOF and/or other DoD assets will work with the host government military and/or LE to capture, assist in capture of, or destroy terrorists. The method may be overt or covert, depending on the relationship with the host government. Extradition or local prosecution will be dependent, once again, on the relationship with the host government. If a host government's prosecution is more likely to be swift and harsh, the US should strongly consider allowing the host government to pursue prosecution.

## NON-PERMISSIVE ENVIRONMENT

A non-permissive environment is one in which the host government is unfriendly or unsupportive of the US war on terrorism. In this situation the CIA and/or SOF would identify, target, and eliminate the terrorists. Unless the US desires to openly confront hostile nations where terrorists operate, a non-permissive environment would limit the operation to a covert ground action in order to maintain an image of plausible deniability; an airborne operation could be traced to the source. Elimination of the terrorist via unconventional warfare to include direct action or any other means necessary to neutralize the target. Operations could also include laser targeting and relaying coordinates for precision bombing but the potential for tracing the action to the US is higher when airborne assets are used. Although abduction is an option it is more difficult to accomplish in a non-permissive environment. Other factors to consider are the potential for collateral damage and the possibility of tracing the action back to the US. Tracing the operation back to the US could have political repercussions and could negatively affect the world opinion of the US.

Another factor in the future war on terrorism is that of competing resources. The primary "combatants" in the low intensity conflict (LIC) war on terrorism are CIA and DoD (SOF). Other agencies (such as NSA and FBI), organizations, and military forces play a role in the coordinated efforts but those roles are more supportive in nature. The CIA and SOF assets will necessarily be stretched over a broad area of operations diluting their ability to effect the war on terrorism unless additional resources are provided.

Of all the resources available to the US the CIA has covert action as a designated responsibility or primary mission.[51] When covert action is required, the CIA has more expertise and capability than the SOF. However, the CIA is more limited in terms of manpower. Conversely, although the DoD SOF can accomplish covert action, that is only one of many missions for which they train, thus they cannot be considered as specializing in covert action. SOF however, has more available manpower. Therefore, the CIA has covert action as a primary mission, but fewer available resources while SOF has more resources, but doesn't specialize in covert actions. A compromise could include the routine melding of SOF and CIA assets and capabilities to provide the most efficient utilization of US resources. Indeed, this was done during OEF but the level of cooperation was probably higher than experienced in the past.

Future non-permissive covert actions will require an extremely small "footprint" with minimal reach back capability in order to avoid detection and maintain a level of plausible deniability. It is extremely important that the action be in no way traceable to the US. In order to best use CT assets, the CIA and SOF will need to combine forces eliminating overlapping capabilities and supporting each other to the maximum extent possible. Some missions may lend themselves to CIA only, some SOF only, while other may require a mixture of both CIA and SOF. Stove-piping of missions and operations will only serve to weaken our ability to attack a more widely spread threat.

**RECOMMENDATIONS**

In the wars traditionally fought by the US, the front was distant from the US homeland. However, the war on terrorism will be fought on three broad (but somewhat overlapping) fronts: the US homeland, abroad, and cyberspace. A traditional war is fought primarily by military and intelligence forces with Federal agencies playing more of a supportive role. The war on terrorism will require active participation by both traditional and non-traditional forces across all levels of the US government. Lessons learned from the war on drugs can be applied to effectively synergize and integrate the whole of the US capabilities across a broad front. The Office of HLS is focused inwardly (vs. abroad) from the strategic to the operational level to protect the US. The newly established Northern Command will also presumably assume some responsibilities for homeland defense. The DCI is focused at the strategic level to advise the President on national intelligence. Finally, the DoD has the traditional role of fighting terrorism abroad (vs. in the homeland). We have a three-front war with no single organization below the level of the National Security Council synergizing the whole of the US capabilities to combat terrorism. As such, there still remain the seams dividing the efforts of the US government. And it is just such seams that the terrorists will seek out and exploit.

To effectively combat terrorism the US needs to make the following changes:

- Organization. Designate the SECDEF as the primary organization for the war on terrorism. The SECDEF has the preponderance of forces, tools, capabilities, manpower, and organizations. Currently, there is no single organization below the level of the NSC coordinating the efforts of the organizations fighting the war on terrorism.
- HLS. Include the SECDEF as a primary member vs. an "invited member" of the HLS Council. The SECDEF has significant resources that can add value to the HLS efforts. Being an invited member does not carry the same level of importance and mandatory participation requisite of a primary member.
- Military. Designate the DoD as the lead organization in fighting the war on terrorism and give the DoD operational control.

- Intelligence. Remove firewalls and stove-pipes between LE and intelligence which inhibit prosecution of the war on terrorism.
- LE. Fully integrate Federal, State, and local LE into the war on terrorism. Minimize encumbrances to LE in executing proactive AT/CT and ensure coordinated efforts throughout all levels of the government.
- Create a standing organization with full spectrum control. Control needs to include more than the traditional military and intelligence sectors; it must integrate Federal, State, and local LE. Control must include adequate resources and budget authority.
- Permanent Organization. Do all this on a permanent (not temporary or ad hoc) basis. A permanent organization will require that all elements work together facilitating and fostering a better relationship both now and in the future. Organizations operating together for a short period of time are more likely to accept levels of friction, work-arounds, and inefficiencies. However, if organizations realize from the beginning that the relationship will be long term they will make a greater effort to get it right from the start.
- Proliferation. Aggressively address sources of WMD to include stockpiles and rogue states.
- Technology. Leverage existing technologies to disseminate information to the "war fighters." Develop technologies to further exploit terrorist weaknesses.
- Congressional Oversight. Congressional oversight is needed to ensure that organizations and agencies are operating efficiently, legally, ethically and to preclude abuses to US citizens.

## CONCLUSION

The terrorist will use any and all means available to attack the US. We cannot guard against every avenue of attack. Therefore, we must organize for a long term war and effectively and efficiently utilize the resources and capabilities we possess, focusing them where and when needed. Technology holds many promising possibilities if we will only allocate the resources necessary to develop them. It should be remembered, however, that technology alone will not win the war. Terrorists will search for and attack our weak points. We must allow our law enforcement agencies to do their job without unnecessary, counterproductive limitations. We must allow the Congressional oversight committees to determine the extent of allowing LE the freedom to monitor communications. We must reorganize to allow coordination of intelligence efforts at the highest levels fostering horizontal and vertical integration. Regarding counterterrorist actions, our intelligence and military organizations must plan for a changing way of fighting terrorism. Finally, the strength and commitment of any policy is ultimately reflected in the funding provided for execution. Funding must be commensurate with the required changes for all agencies.

We are making progress in the war on terrorism. This is primarily due to the American will and innovative spirit. However, will and innovation can only produce limited effects in a long term campaign. We must set in place permanent organizations and relationships which facilitate efficient, effective operations and remove seams which the terrorists seek to exploit.

Fighting terrorism is a way of life for the foreseeable future. If we are going to live in relative safety, there will be a price to pay. If we are not willing to pay the price we may well devolve to the situation experienced on a daily basis in Middle East and other areas. The US can win the war on terrorism. We are moving in the right direction. However, we need to continue to make changes in the ways, ends, and means of our National Security Strategy and we need to do it while there is sufficient momentum, before the memory of 11 September 2001 is lost to the next crisis.

WORD COUNT = 8,824

## ENDNOTES

[1] George W. Bush, "President Signs Authorization for Use of Military Force Bill," 18 September 2001; available from http://whitehouse.gov/news/releases/2001/09/20010918-10.html; Internet; accessed 24 February 2002.

[2] Legal Information Institute, "US Code Collection," available from http://www4.law.cornell.edu/uscode/22/2656f.html; Internet; accessed 26 September 2001.

[3] U.S. Department of State, Patterns of Global Terrorism – 2000 (Washington, D.C: U.S. Department of State, April 2001); available from http://state.gov/s/ctrls/pgrpt/2000/index.cfm?docid=2419; Internet; accessed 26 September 2001.

[4] U.S. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02 (Washington, D.C.: U.S. Joint Chiefs of Staff, 12 April 2001), 428.

[5] Carl Von Clausewitz, On War, ed. and trans. Michael Howard and Peter Paret (Princeton: Princeton University Press, 1984), 75.

[6] White House, "Presidential Decision Directive 39 – U.S. Policy on Counterterrorism," 21 June 1995; available from http://fas.org.irp/offdocs/pdd39.htm; Internet; accessed 10 September 2001.

[7] Patterns of Global Terrorism – 2000.

[8] U.S. Joint Chiefs of Staff Publication 1-02, 31.

[9] U.S. Joint Chiefs of Staff, Joint Doctrine Encyclopedia, (Washington, D.C.: U.S. Joint Staff, 16 July 1997), 39.

[10] U.S. Joint Chiefs of Staff Publication 1-02, 104.

[11] Joint Doctrine Encyclopedia, 207.

[12] John M. Shalikashvili, National Military Strategy of the United States of America, Shape, Respond, Prepare Now: A Military Strategy for a New Era (Washington, D.C.: U.S. Joint Chiefs of Staff, 12 April 2001), 9.

[13] Brian Sheridan, "Statement by Brian Sheridan Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, Before the Senate Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services, 106th Cong.," 24 March 2000; available from http://www.fas.org/spp/starwars/congress/2000_h/000324-sheridan.htm; Internet; accessed 25 March 2002.

[14] Kathleen T. Rhem, "Technology Makes it Easier for Rogue States to get Anthrax," Pentagram, 1 March 2002; available from http://www.dcmilitary.com/army/pentagram/7_08/national_news/14555-1.html; Internet; accessed 23 March 2002.

[15] Fred Guterl and Eve Conant, "In the Germ Labs," Newsweek, 25 February 2002; available from https://ca.dtic.mil/cgi-bin/ebird.cgi?doc_url=Feb2002/s2002022germ.htm; Internet: accessed 22 February 2002.

[16] ibid.

[17] ibid.

[18] ibid.

[19] Jeffrey Kluger, "The Nuke Pipeline," Time 158 (17 December 2001): 40-45 [database on-line]; available from UMI ProQuest, Bell & Howell; accessed 1 January 2002.

[20] John Pike, "Nuclear Weapons Design," 21 October 1998; available from http://www.fas.org/nuke/intor/nuke/design.htm; Internet; accessed 25 March 2002.

[21] Bill Nichols and Peter Eisler, "The Threat of Nuclear Terror is Slim But Real," USA Today 20 (29 November 2001): A1 [database on-line]; available from UMI ProQuest, Bell & Howell. Accessed 1 January 2002.

[22] David E. Kaplan and Douglas Pasternak, "Terror's Dirty Secret: Radioactive Material, Loosely Guarded, Makes a Cheap Weapon," U.S. News and World Report 131 (3 December 2001): 26-28 [database on-line]; available from UMI ProQuest, Bell & Howell. Accessed 1 January 2002.

[23] ibid.

[24] Nichols.

[25] H.R. 3162, "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001," 24 October 2001; available from http://thomas.loc.gov//cgiibin/bdquery/z?d107:HR03162@@@D&summ2=m&; Internet; accessed 19 January 2002.

[26] Scott Shane, "Secret U.S. Court Handed New Power to Fight Terror," Baltimore Sun, 29 October 2001; available from http://www.sunspot.net/news/custom/attack/; Internet; accessed 23 February 2002.

[27] George W. Bush, "Fact Sheet on Terrorist Financing Executive Order," 24 September 2001; available from http://www.whitehouse.gov/news/releases/2001/09/20010924-2.html, Internet; accessed 7 October 2001.

[28] ibid.

[29] ibid.

[30] Paul O'Neill, "Remarks by Treasury Secretary Paul O'Neill on New Terrorist Financing Designations," 26 February 2002; available from http://treas.gov//press/releases/po1047.htm; Internet; accessed 23 March 2002.

[31] George W. Bush, "Financial Actions in the War on Terrorism," available from http://www.whitehouse.gov/response/text/financialresponse.html; Internet; accessed 23 March 2002.

[32] Richard A. Best, Jr., Intelligence and Law Enforcement: Countering Transnational Threats to the U.S., Washington, D.C.: Library of Congress, Congressional Research Service, 3 December 2001.

[33] George W. Bush, "President Establishes Office of Homeland Security," 8 October, 2001; available from http://www.whitehouse.gov/news/releases/2001/10print/20011008.html; Internet; accessed 17 March 2002.

[34] ibid.

[35] ibid.

[36] ibid.

[37] George W. Bush, "Securing the Homeland, Strengthening the Nation," available from http://www.whitehouse.gov/homeland/homeland_security_book.html; Internet; accessed 25 February 2002.

[38] George W. Bush, "Homeland Security Budget," available from http://www.whitehouse.gov/homeland/homeland_security_charts.html; Internet; accessed 25 February 2002.

[39] James V. Grimaldi, Steve Fainaru, and Gilbert M. Gaul, "Losing Track of Illegal Immigrants; Once in U.S., Most Foreigners Easily Escape Notice of INS," Washington Post, (7 October 2001); sec. A, p. 1.

[40] ibid.

[41] Bob Sullivan, "Warming to Big Brother," 14 November 2001; available from http://www.infowar.com/class_1/01/class1_111501a_jshtml; Internet; accessed 6 January 2002.

[42] Grimaldi.

[43] ibid.

[44] ibid.

[45] U.S. Department of Justice, Immigration and Naturalization Service, "INS Restructuring Plan," 14 November 2001; available from http://www.ins.usdoj.gov/graphics/publicaffairs/factsheets/restruct.htm; Internet; accessed 25 February 2002.

[46] Abram Shulsky, Silent Warfare (Washington, DC: Brassey's, 1993), 179.

[47] Shane.

[48] Walter Pincus, "Congressional Panels Join to Probe U.S. Intelligence," Washington Post, 12 February 2002, sec. A, p. 1.

[49] Shulsky, 184.

[50] Shulsky, 186.

[51] Ronald Reagan, "Executive Order 12333: United States Intelligence Activities," 4 December 1981; available from http://www.fas.org/irp/offdocs/eo12333.htm; Internet; accessed 25 February 2002.

## BIBLIOGRAPHY

Best, Richard A., Jr. Intelligence and Law Enforcement: Countering Transnational Threats to the U.S. Washington, D.C.: Library of Congress, Congressional Research Service, 3 December 2001.

Bush, George W. "Fact Sheet on Terrorist Financing Executive Order." 24 September 2001. Available from http://www.whitehouse.gov/news/releases/2001/09/20010924-2.html. Internet. Accessed 7 October 2001.

Bush, George W. "Financial Actions in the War on Terrorism." Available from http://www.whitehouse.gov/response/text/financialresponse.html. Internet. Accessed 23 March 2002.

Bush, George W. "Homeland Security Budget." Available from http://www.whitehouse.gov/homeland/homeland_security_charts.html. Internet. Accessed 25 February 2002.

Bush, George W. "President Establishes Office of Homeland Security." 8 October 2001. Available from http://www.whitehouse.gov/news/releases/2001/10print/20011008.html. Internet. Accessed 17 March 2002.

Bush, George W. "President Signs Authorization for Use of Military Force Bill." 18 September 2001. Available from http://whitehouse.gov/news/releases/2001/09/20010918-10.html. Internet. Accessed 24 February 2002.

Bush, George W. "Securing the Homeland, Strengthening the Nation." Available from http://www.whitehouse.gov/homeland/homeland_security_book.html. Internet. Accessed 25 February 2002.

Grimaldi, James V., Steve Fainaru, and Gilbert M. Gaul. "Losing Track of Illegal Immigrants; Once in U.S., Most Foreigners Easily Escape Notice of INS." Washington Post, 7 October 2001, sec. A, p. 1.

Guterl, Fred, and Eve Conant. "In the Germ Labs." Newsweek, 25 February 2002. Available from https://ca.dtic.mil/cgi-bin/ebird.cgi?doc_url=Feb2002/s2002022germ.htm. Internet. Accessed 22 February 2002.

H.R. 3162. "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001." 24 October 2001. Available from http://thomas.loc.gov//cgiibin/bdquery/z?d107:HR03162@@@D&summ2=m&. Internet. Accessed 19 January 2002.

Kaplan, David E., and Douglas Pasternak. "Terror's Dirty Secret: Radioactive Material, Loosely Guarded, Makes a Cheap Weapon." U.S. News and World Report 131 (3 December 2001): 26-28. Database on-line. Available from UMI ProQuest, Bell & Howell. Accessed 1 January 2002.

Kluger, Jeffrey. "The Nuke Pipeline." Time 158 (17 December 2001): 40-45. Database on-line. Available from UMI ProQuest, Bell & Howell. Accessed 1 January 2002.

Legal Information Institute. "US Code Collection." Available from http://www4.law.cornell.edu/uscode/22/2656f.html. Internet. Accessed 26 September 2001.

Nichols, Bill, and Peter Eisler. "The Threat of Nuclear Terror Is Slim But Real." USA Today 30 (29 November 2001): A1. Database on-line. Available from UMI ProQuest, Bell & Howell. Accessed 1 January 2002.

O'Neill, Paul. "Remarks by Treasury Secretary Paul O'Neill on New Terrorist Financing Designations." 26 February 2002. Available from http://treas.gov//press/releases/po1047.htm. Internet. Accessed 23 March 2002.

Pike, John. "Nuclear Weapons Design." 21 October 1998. Available from http://www.fas.org/nuke/intor/nuke/design.htm. Internet. Accessed 25 March 2002.

Pincus, Walter. "Congressional Panels Join to Probe U.S. Intelligence." Washington Post, 12 February 2002, sec. A, p. 1.

Reagan, Ronald. "Executive Order 12333: United States Intelligence Activities." 4 December 1981. Available from http://www.fas.org/irp/offdocs/eo12333.htm. Internet. Accessed 25 February 2002.

Rhem, Kathleen T. "Technology Makes it Easier for Rogue States to get Anthrax," Pentagram, 1 March 2002. Available from http://www.dcmilitary.com/army/pentagram/7 08/national news/14555-1.html. Internet. Accessed 23 March 2002.

Shalikashvili, John M. National Military Strategy of the United States of America, Shape, Respond, Prepare Now: A Military Strategy for a New Era. Washington, D.C.: U.S. Joint Chiefs of Staff, 12 April 2001.

Shane, Scott. "Secret U.S. Court Handed New Power to Fight Terror." Baltimore Sun, 29 October 2001. Available from http://www.sunspot.net/news/custom/attack/. Internet. Accessed 23 February 2002.

Sheridan, Brian. "Statement by Brian Sheridan Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, Before the Senate Subcommittee on Emerging Threats and Capabilities of the Committee on Armed Services, 106th Cong." 24 March 2000. Available from http://www.fas.org/spp/starwars/congress/2000 h/000324-sheridan.htm. Internet. Accessed 25 March 2002.

Shulsky, Abram. Silent Warfare. Washington, DC: Brassey's, 1993.

Sullivan, Bob. "Warming to Big Brother." 14 November 2001. Available from http://www.infowar.com/class 1/01/class1 111501a jshtml. Internet. Accessed 6 January 2002.

U.S. Department of Justice, Immigration and Naturalization Service. "INS Restructuring Plan." 14 November 2001. Available from http://www.ins.usdoj.gov/graphics/publicaffairs/factsheets/restruct.htm. Internet. Accessed 25 February 2002.

U.S. Department of State. Patterns of Global Terrorism – 2000. Washington, D.C: U.S. Department of State, April 2001. Available from http://state.gov/s/ctrls/pgrpt/2000/index.cfm?docid=2419. Internet. Accessed 26 September 2001.

U.S. Joint Chiefs of Staff. Department of Defense Dictionary of Military and Associated Terms. Joint Publication 1-02. Washington, D.C.: U.S. Joint Chiefs of Staff, 12 April 2001.

U.S. Joint Chiefs of Staff. Joint Doctrine Encyclopedia. Washington, D.C.: U.S. Joint Chiefs of Staff, 16 July 1997.

Von Clausewitz, Carl. On War. Edited and translated by Michael Howard and Peter Paret. Princeton: Princeton University Press, 1984.

White House. “Presidential Decision Directive 39 – U.S. Policy on Counterterrorism.” 21 June 1995. Available from http://fas.org.irp/offdocs/pdd39.htm. Internet. Accessed 10 September 2001.